**March 5, 2024**

Collin received an email that a new user was added to our website ghmpodcast.com (Production). He checked the users on the WordPress (WP) dashboard and found four suspicious users on the site:

|  |  |  |  |
| --- | --- | --- | --- |
| **Username** | **Name** | **Email** | **Role** |
| admin@zzna.ru |  | admin@zzna.ru | Adminstrator |
| samuelthompsonc53 |  | samuelthompsonc53@outlook.com | None |
| wpadminne |  | sewtgresh@wsv.com | Adminstrator |
| wpsupp-user | wp-needuser | wpsupp-user@word.com | Adminstrator |

Collin also found the following plugin installed on the website visible on the WP dashboard that none of us (IT Webmasters) had installed. This plugin was not in the test version of this site either.

* WP Console: <https://wordpress.org/plugins/wp-console/>

After installing the security plugin Wordfence, we ran a scan of the website and found two additional mysterious plugins that contained files Wordfenced reported as malicious with “Critical” issue warnings. The details on all these files said, “This file appears to be installed or modified by a hacker to perform malicious activity.”

Weirdly, the plugins where these files were contained (wordpress-jseo and wp-cleansong) were not visible on the WP dashboard but were visible server-side. They contained these files reported as malicious by Wordfence:

* /var/www/ghmpodcast/wp-content/plguins/wordpress-jseo/da2.2.php
* /var/www/ghmpodcast/wp-content/plugins/wp-cleansong/plane.php
* /var/www/ghmpodcast/wp-content/plugins/wp-cleansong/wp-cleansong.php
* /var/www/ghmpodcast/wp-content/plugins/wordpress-jseo/wp-admins.php

The Wordfence scan also gave a warning for the plugin “Podcast Subscribe Buttons” (a plugin we actually use) with a “Critical” issue warning, saying, “You need to upgrade “Podcast Subscribe Buttons” to the newest version to ensure you have any security fixes the developer has released.” Chris Sanford reviewed the plugin’s changelog and found this plugin was most likely the entry point for the hackers to breach the site.

Several other plugins needed updating, although none came back with “Critical” issues reported by Wordfence. All these plugins were updated. While “Podcast Subscribe Buttons” was the most likely culprit, it is possible the breach could have occurred on any of these outdated plugins.

All suspicious users were removed, and the roles of current users with “Adminstrator” status (Chris Blackburn and Jeremiah Wentz) were set to “No role for this site,” temporarily disabling their roles on the website. The three plugins installed by the hackers (wp-console, wp-cleansong, and wordpress-jseo) were also removed. The Podcast Subscribe Buttons plugin was updated to the latest version.

Nicole installed Wordfence on all our websites, ran scans, and found no “Critical” issues reported.

Later in the day, Collin received another email that a new user registration was created on the WP website everydayeducatorpodcast.com (Production) with the following credentials:

|  |  |  |  |
| --- | --- | --- | --- |
| **Username** | Name | **Email** | **Role** |
| Bury |  | [b@p.com](mailto:b@p.com) | Adminstrator |

Collin immediately removed the user. We ran a Wordfence scan of the website, and no “Critical” issues were reported. No malicious plugins or files were found. Some plugins needed updating (like on ghmpodcast.com, with no “Critical” issues reported by Wordfence) and were all updated to the latest versions.

**March 6, 2024**

First thing in the morning, we scanned both previously infected sites with Wordfence (ghmpodcast.com and everydayeducatorpodcast.com). everydayeducatorpodcast.com reported no “Critical” issues. ghmpodcast.com, however, reported several warnings with “Critical” issues.

There were about 6-8 files reported as having malicious code. I don’t have a record of all these files’ names. However, all but one of them were within the default WP themes directories that are installed on every WP website. These themes were inactive since the website uses a different theme. The one exception was a file that was in the root directory of the website:

* /var/www/ghmpodcast/wp-staie.php

On the WP dashboard, we deleted all the default WP themes from the website (thereby also deleting the malicious files that were found within these themes’ directories).

Server-side, Bayardo found two additional suspicious files (named all.php and yuao.php). One of the files contained code that appeared to enable users to be directly added to the website’s database.

Bayardo removed all these malicious files (wp-staie.php, all.php, and yuao.php). He installed ClamAV (antivirus and antimalware software), scanned the ghmpodcast.com website, and found no malware or viruses.

We also re-ran a Wordfence scan of ghmpodcast.com on the WP dashboard, and no warnings with “Critical” issues were reported.